Biometrics

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

论文讲解

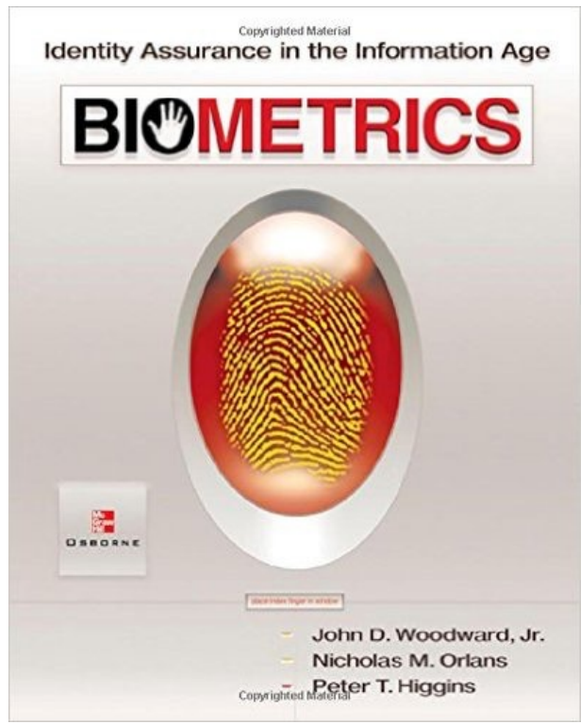
第一组

口令回顾

1 身份认证	2 其余机制	3 口令泄漏	4 其余
• 身份认证 • 认证因子 • OTP • PKI	• 口令管理 • SSO • OpenID,OAuth • 新口令模型	• SAuth • PolyPassHash • Honeyword • HoneyHash	• SlidePIN • 图形口令 • 图形口令评价

本次课程内容

- 生物学认证简介
- 生物学认证系统
- 生物学认证类型
- 生物学认证挑战
- 生物学认证验活



生物学认证简介

身体作为口令

定义

- **根据生理和行为特征来识别或验证一个有生命个体的自动方法**

- 指纹
- 手型
- 脸型
- 虹膜
- 视网膜
- 耳朵
- 静脉
- 脸部热成像
- *DNA*

生理

vs

行为

识别 *vs* 验证

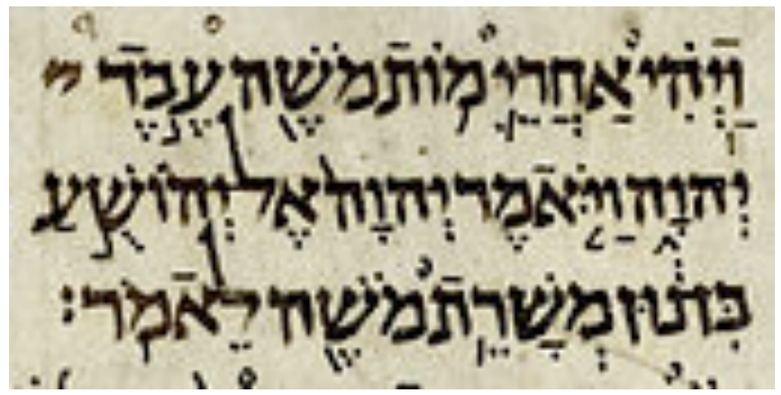
有生命

自动

- 语音
- 签名
- 步态
- 击键
- 滑动
- 握手
- 足部运动
- 操作行为
- 脑电波

历史

Gilead then cut Ephraim off from the fords of the Jordan, and whenever Ephraimite fugitives said, 'Let me cross,' the men of Gilead would ask, 'Are you an Ephraimite?' If he said, 'No,' they then said, 'Very well, say "Shibboleth" (שבלת).' If anyone said, "Sibboleth" (סבלת), because he could not pronounce it, then they would seize him and kill him by the fords of the Jordan. Forty-two thousand Ephraimites fell on this occasion.
—Judges 12:5-6, NJB



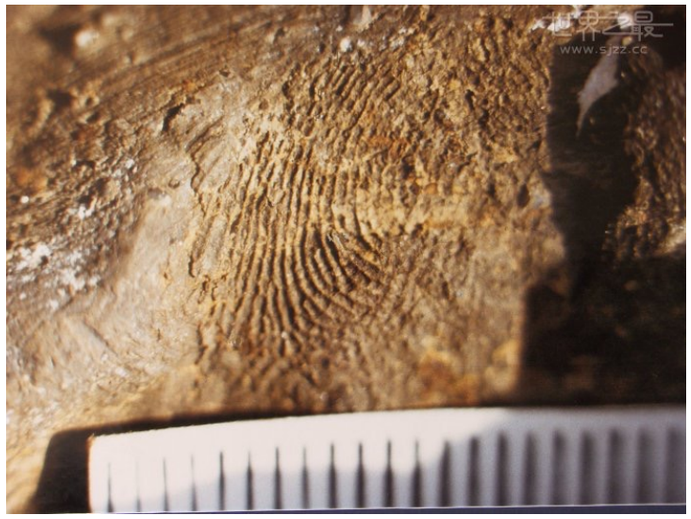
45000厄弗雷姆人

《士师记》 （*The Book of Judges*）

Shibboleth
A Project of the Internet2 Middleware Initiative

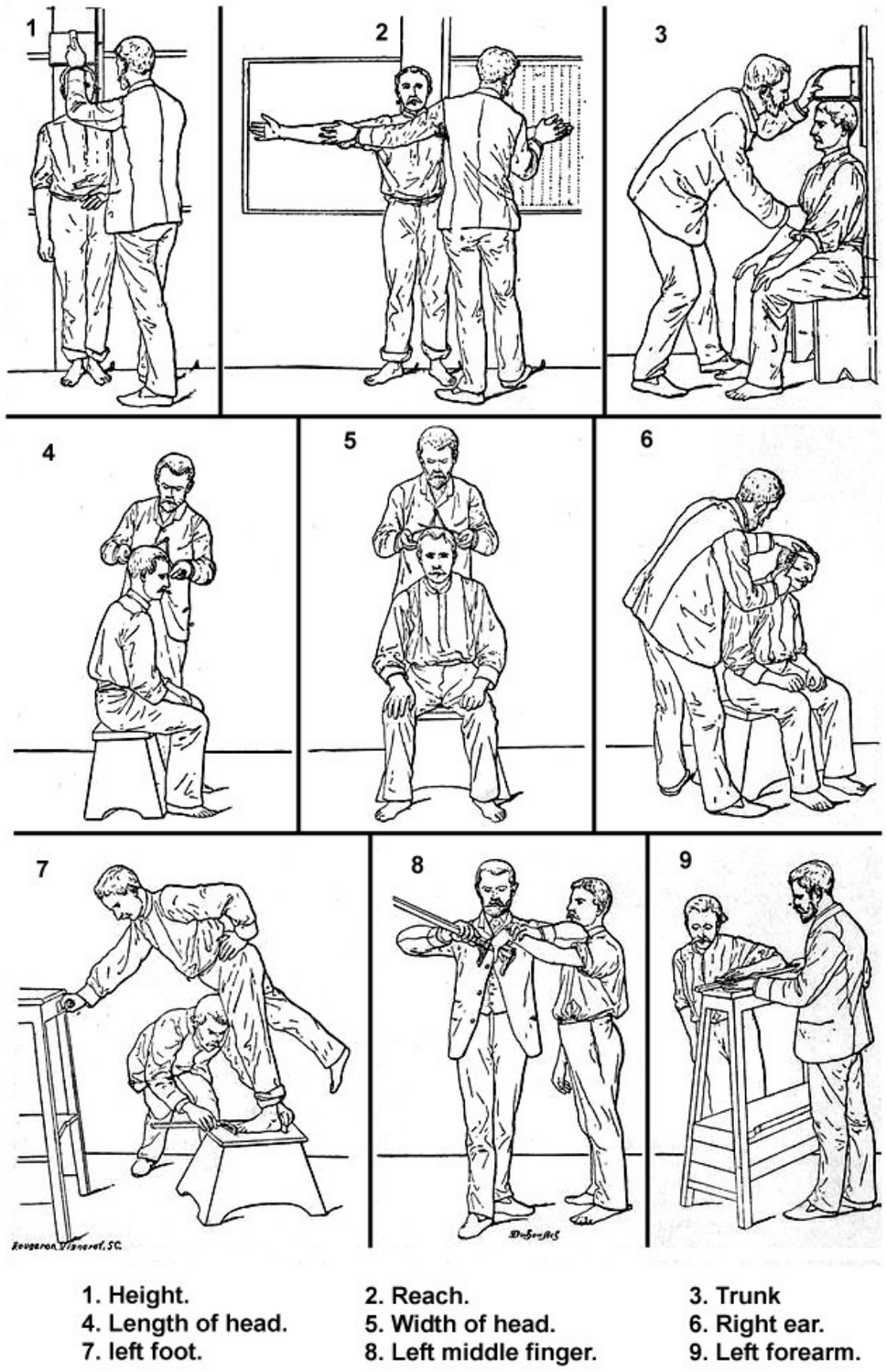
http://shibboleth.internet2.edu/

历史



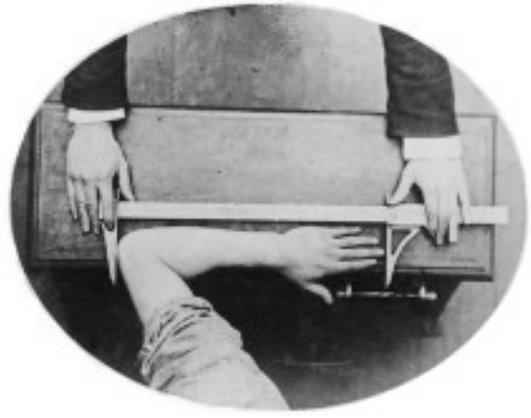
7000年前 半坡遗址

1880 Nature Henry Faulds

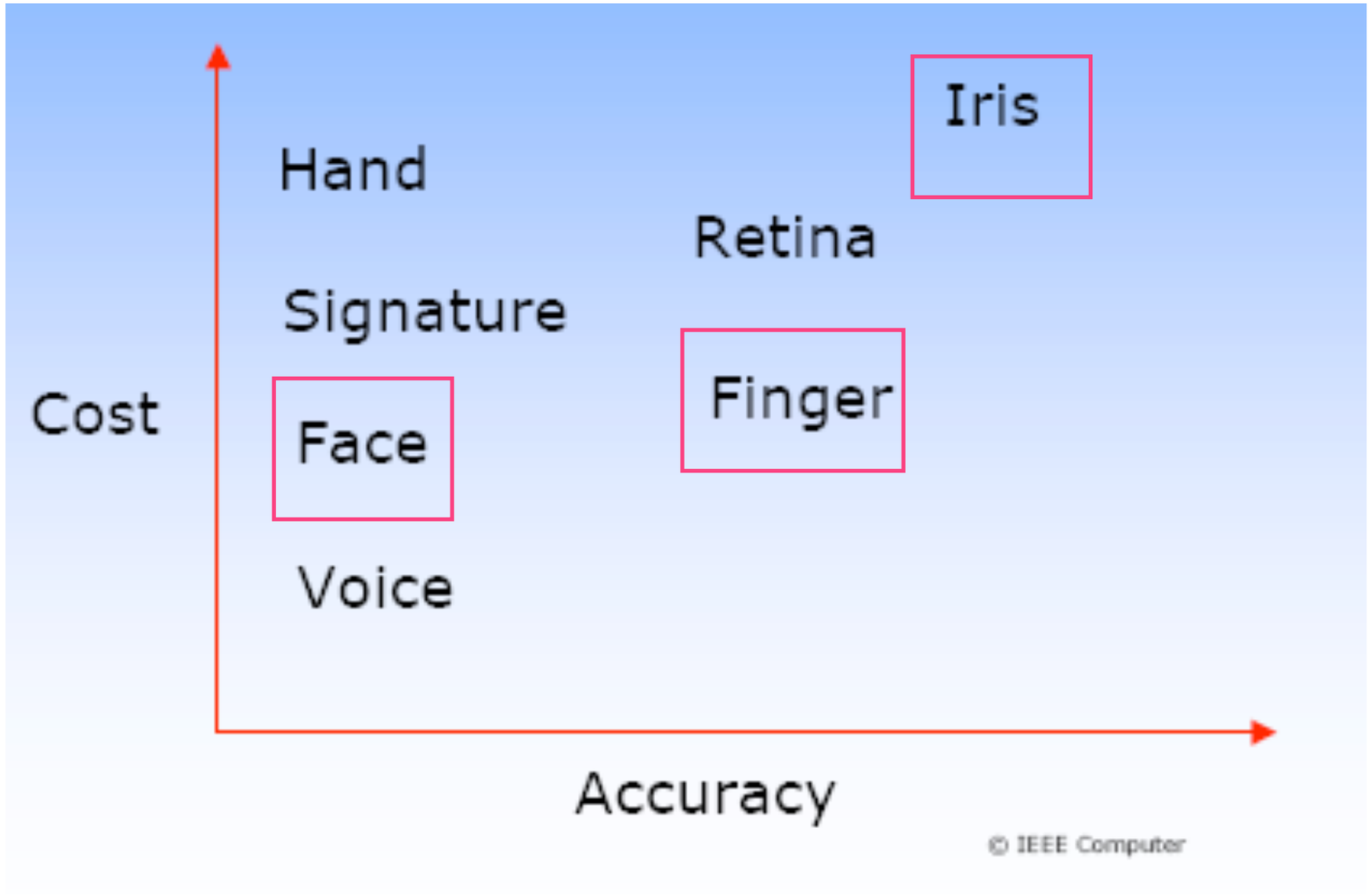


1. Height.
2. Reach.
3. Trunk
4. Length of head.
5. Width of head.
6. Right ear.
7. left foot.
8. Left middle finger.
9. Left forearm.

1882 Bertillion系统



现状



1963: 指纹　***1963:*** 语音　***1966:*** 脸型　***1971:*** 手型　***1987:*** 虹膜

2003: US-Visit

应用

物理访问控制

出入境

金融支付

背景调查

- 身份证件
- 军事应用
- 社会公益
- 考勤
- 赌场
- 计算机和网络
- 智能手机
- 个性化

优缺点

优点

- 安全
- 方便
- 难于欺骗，不容易改变、丢失、复制
- 唯一性标识
- 被动标识

缺点

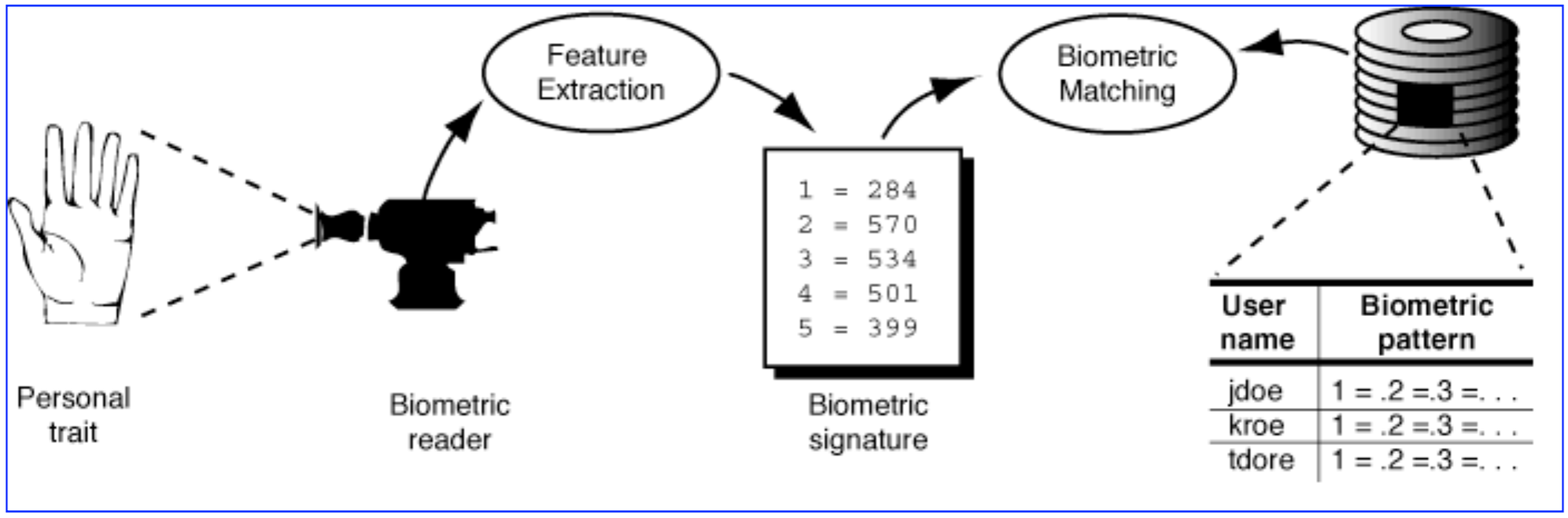
- 准确性
- 难于作废
- 存在适配问题
- 可能侵犯隐私
- 系统存在被攻击的危险

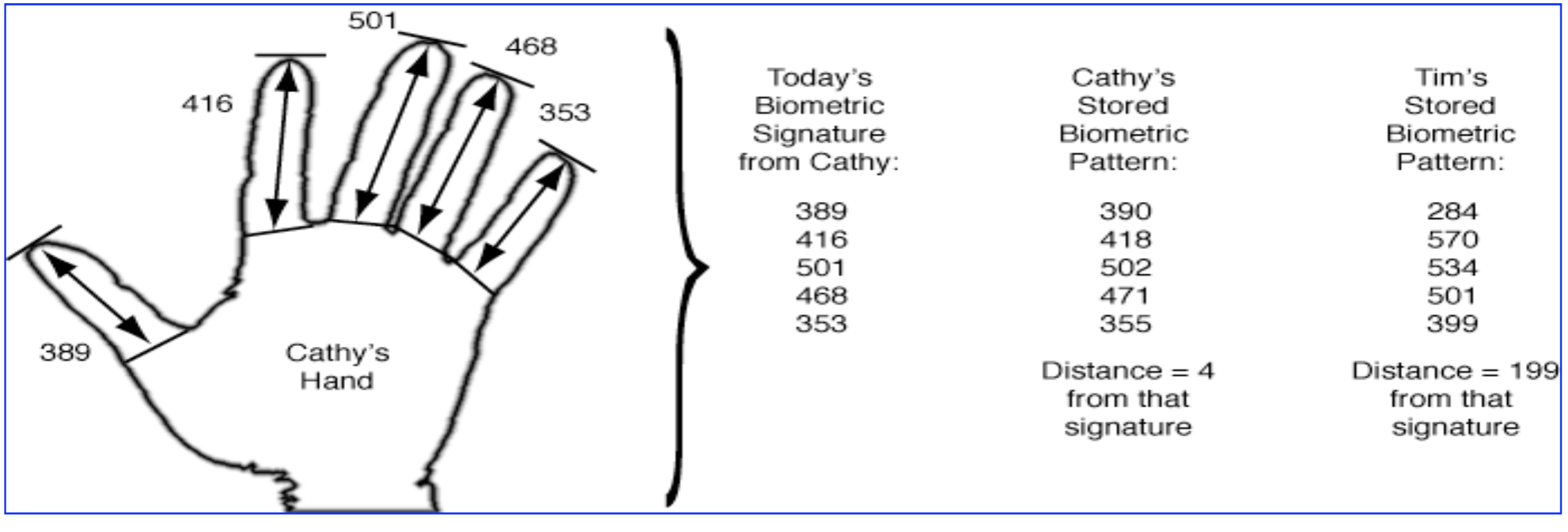
911的影响

挑战

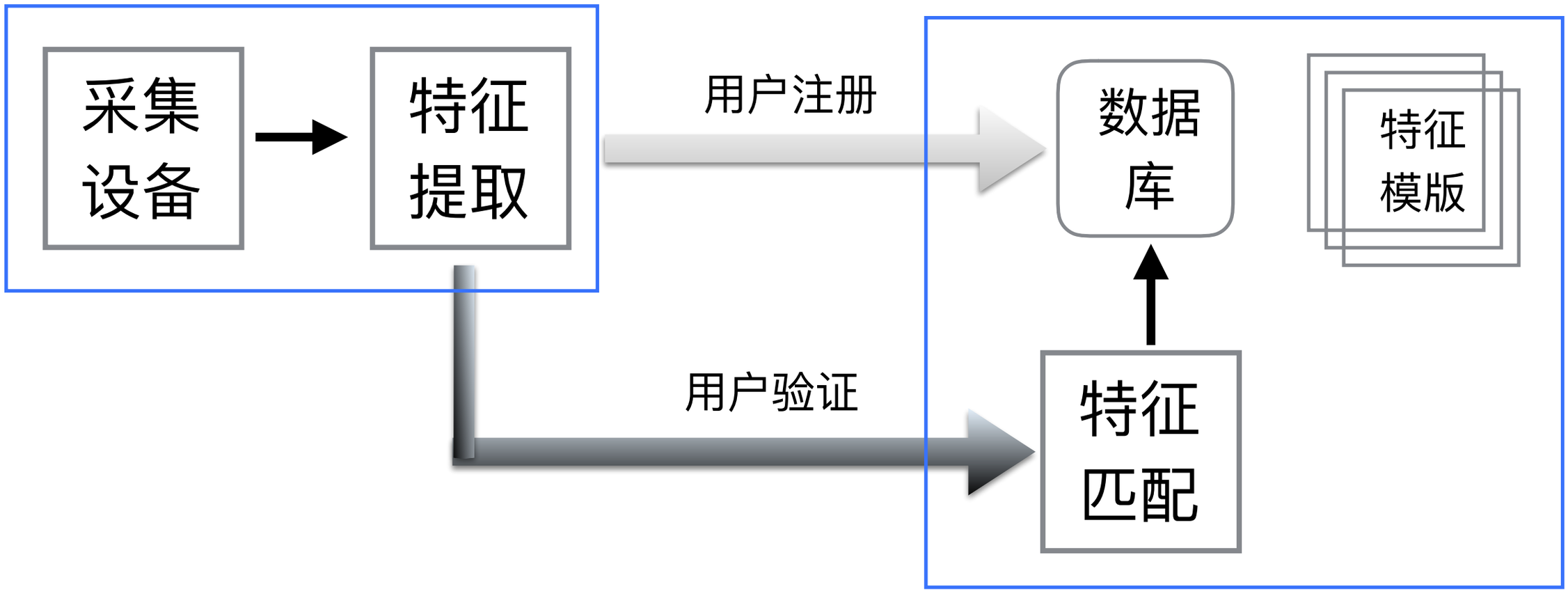
生物学认证系统

例子


Feature Extraction
Biometric Matching
1 = 284
2 = 570
3 = 534
4 = 501
5 = 399
User name
Biometric pattern
jdoe
1 = .2 =.3 =. . .
kroe
1 = .2 =.3 =. . .
tdore
1 = .2 =.3 =. . .
Personal trait
Biometric reader
Biometric signature


501
468
416
353
389
Cathy's Hand
Today's Biometric Signature from Cathy:
389
416
501
468
353
Cathy's Stored Biometric Pattern:
390
418
502
471
355
Distance = 4 from that signature
Tim's Stored Biometric Pattern:
284
570
534
501
399
Distance = 199 from that signature

构成



生物特征

- 健壮性 (持久性)
  - ✴ 能够在相当长时间内反复表现出来，并让生物认证系统成功进行自动测量的性质
- 独特性 (唯一性)
  - ✴ 人与人之间存在足够大的差异，并且这种差异能够被测量出来
  - ✴ 所有的生物特征都包括三种因素
    - ➡ 遗传因素：天生
    - ➡ 表现因素：胚胎发育的早起形成
    - ➡ 行为因素：后天学习的行为，可以改变和重新学习

注册

- 模板生成
  - ✳ 单个和多个生物特征样本
  - ✳ 生物特征类型、用户和环境因素、性能要求
  - ✳ 指纹
    - ➡ 手指放在扫描仪上的角度和位置
    - ➡ 手指上伤痕、残留物、障碍物
    - ➡ 扫描仪的灰尘和残留物
- 注册分数：反应注册质量
- 强制 vs 自愿
- 动态阀值 vs 静态阀值

多重注册

注册失败率
允许的次数
需要的附加信息
注册数据的存储位置
是否需要多方法的注册

模版管理

- 模板：通过原始数据提取出来的生物特征的总和
- 模板的老化和漂移
- 模板更新
- 模板存储
  - ✴ 空间
  - ✴ 方式：本地、网络、便携设备
- 模板安全

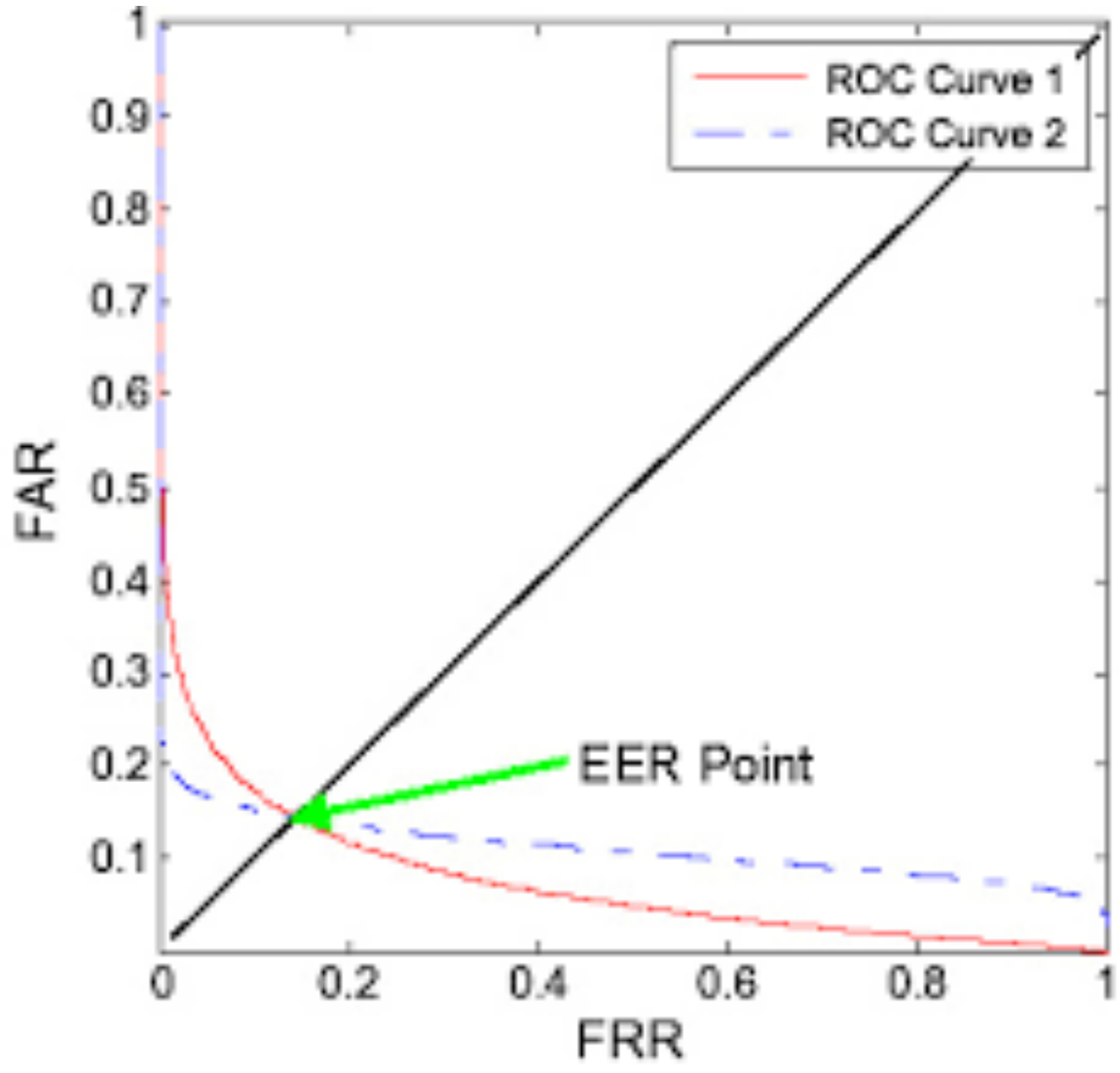
所有生物认证系统的有效性是以模版数据库的质量和完备性为基础的，因为每一次匹配均需要将获得的数据和存储的参考模版相比较

匹配算法

- 验证：一对一匹配、肯定性匹配
- 识别：一对多匹配、否定性匹配
- 合作 vs 非合作
- 活体检测
  - ✴ 热传感器测量体热
  - ✴ 测量身体运动或者其它特征
  - ✴ 费用和性能
  - ✴ 不要以为生物学认证设备会做活体检测

性能指标

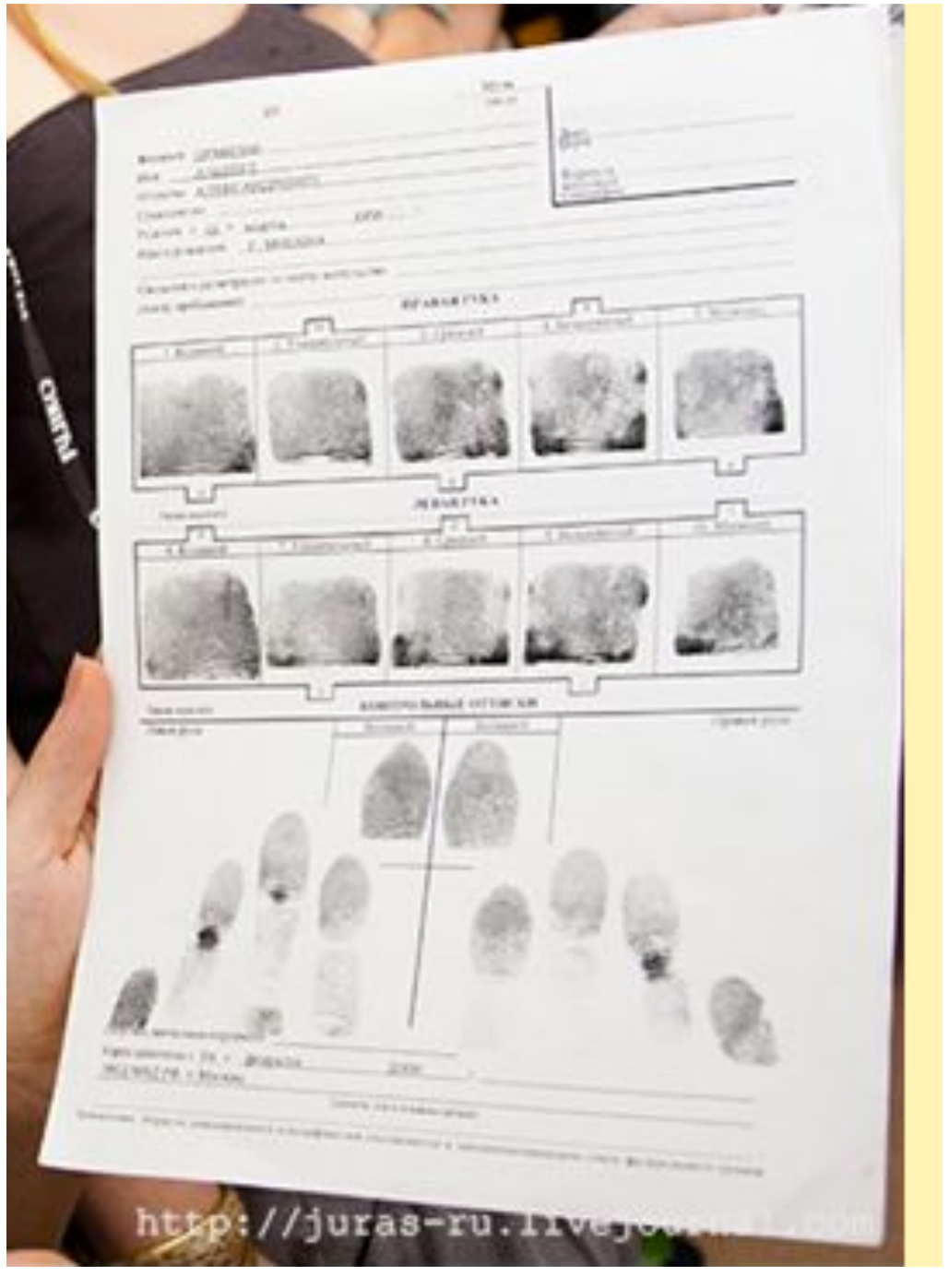
- FAR: False Acceptance Rate
- FRR: False Rejection Rate
- ERR: Equal Error Rate
- ROC: Receiver Operating Characteristic
- AUC: Area Under the Curve of ROC



生物学认证类型

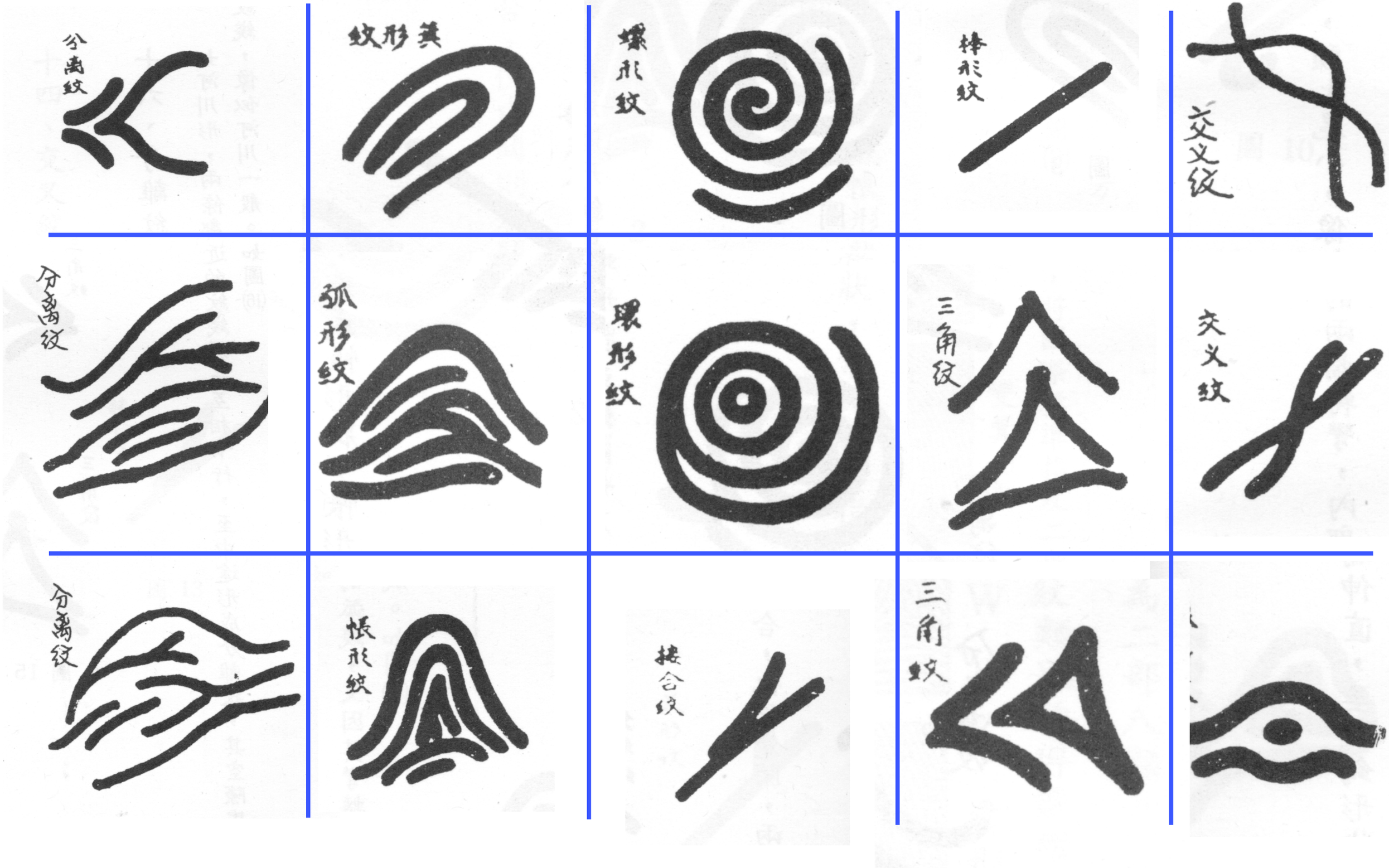
Types of Biometrics

指纹



Types of Biometrics

指纹



Types of Biometrics

指纹

环
弧
螺旋

末梢
分叉
园点
组合

总体形状

突起细节和路径

单个突起细节

Types of Biometrics

指纹

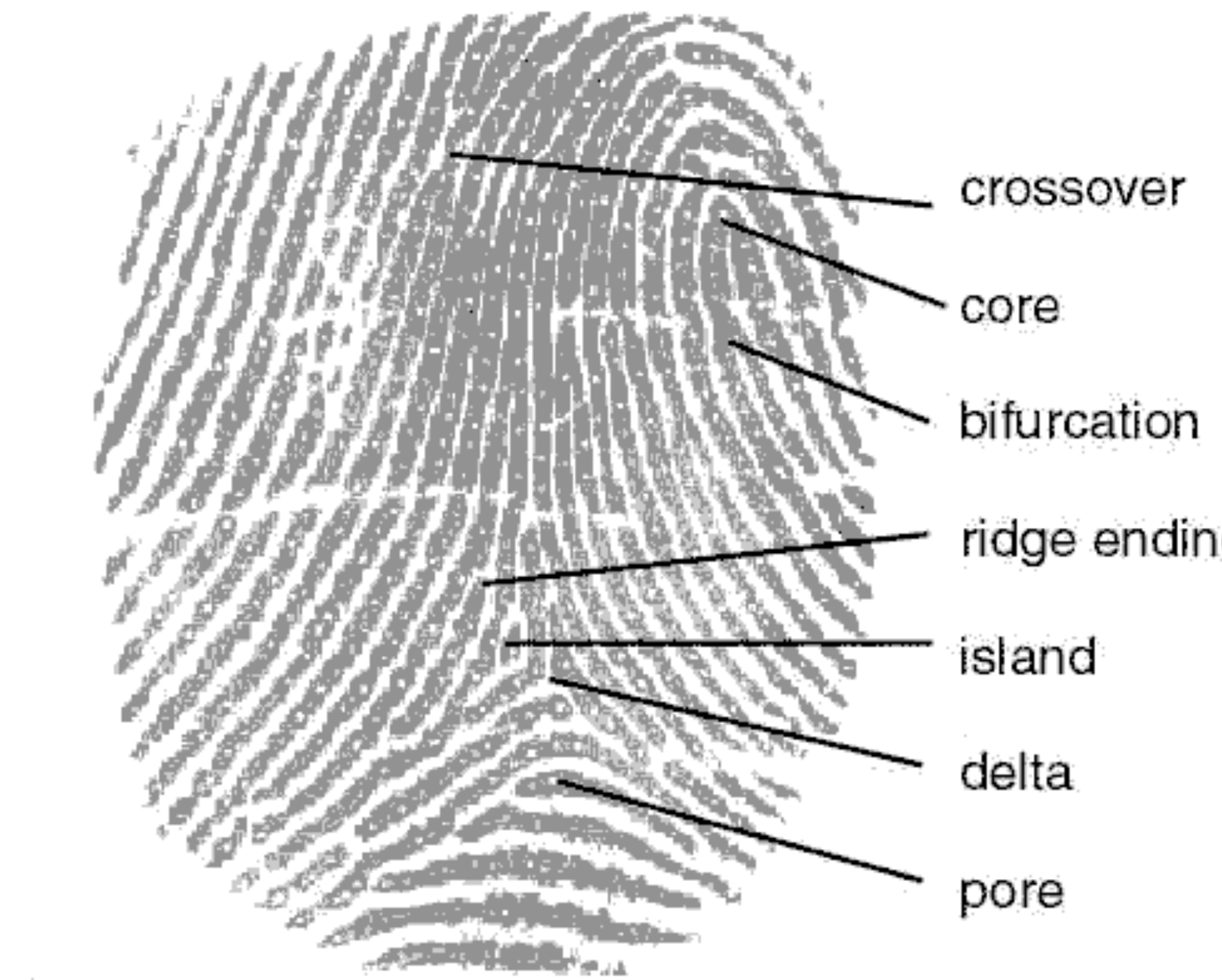


Figure 1

http://www.biocn.com/serv-finger.htm

亨利系统将一个指纹的图形划分为：左环，右环，拱，涡和棚状拱。环型占了将近2/3的指纹图象，涡占1/3，可能存在5-10%的拱，这种指纹图形分类方法在大规模刑侦上有着广泛运用，但在生物识别认证方面很少有运用。

crossover 交叉

core核

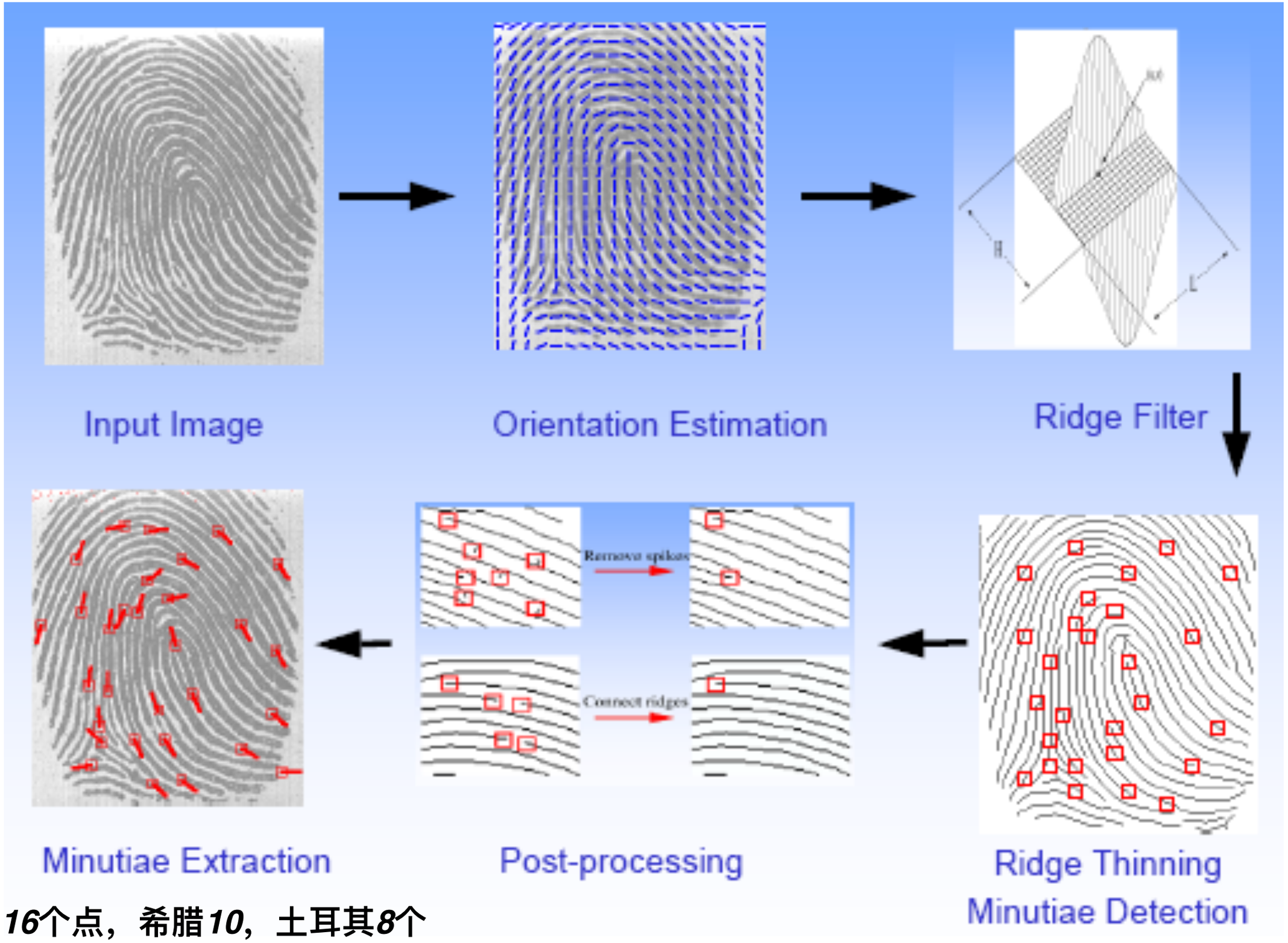
bifurcation分岔

ridge ending脊断点

island 岛型区域

delta三角形区域 pore孔

指纹



英国*16*个点，希腊*10*，土耳其*8*个

Types of Biometrics

手机上指纹的历史

西门子

1998

背部

刮擦式

SAGEM
MC 959

2000

富士通

2003

Synaptics™

GOODiX 创新技术 丰富生活

FINGERPRINTS

AuthenTec

光学 *vs* 电容

前置 *vs* 后置

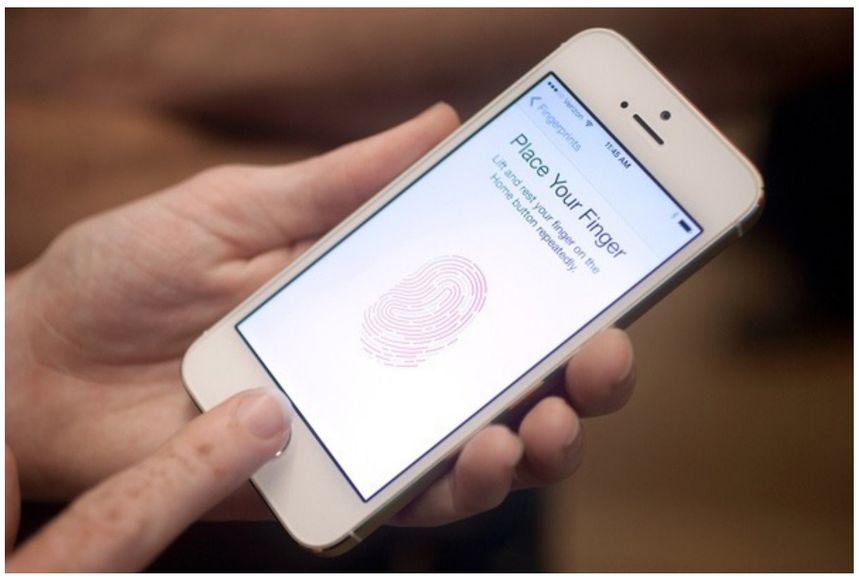
Moto
MB 860

2013，2.5亿

Synaptics

validity™

2012，3.7亿



Types of Biometrics

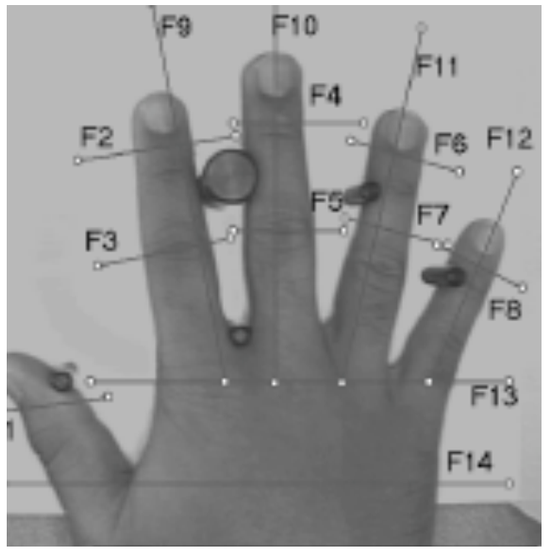
攻击指纹

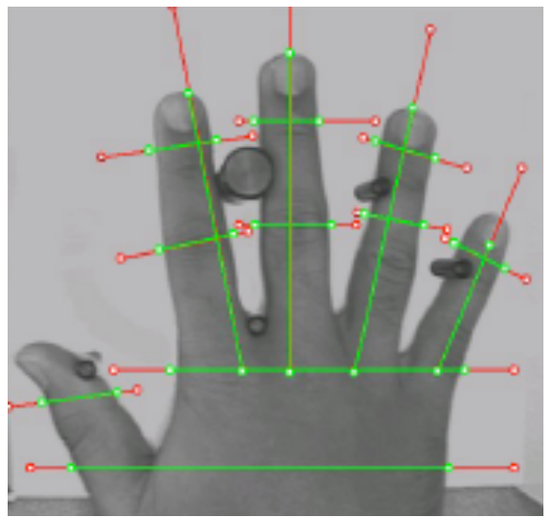
Types of Biometrics

手型

手指：

- 长度
- 宽度
- 厚度
- 表面区域





访问控制

资源使用

打卡

尺寸

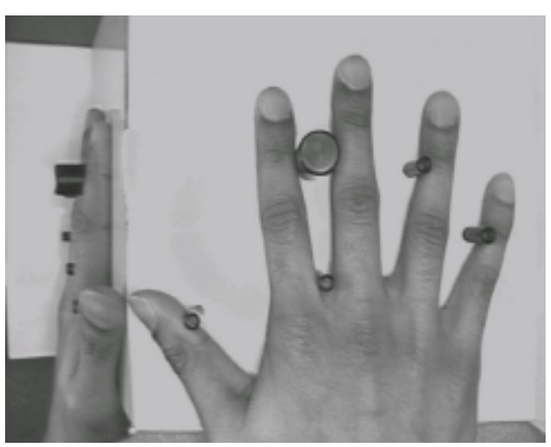
结合掌纹

AirAuth

美国INS

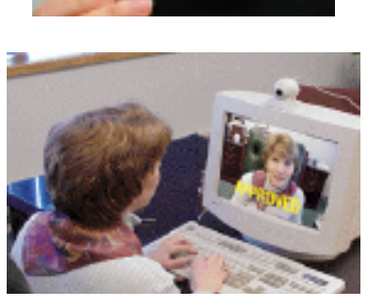
佐治亚大学

奥兰多迪斯尼乐园



脸型

识别和验证身份
监视和监控
视频搜索和索引应用



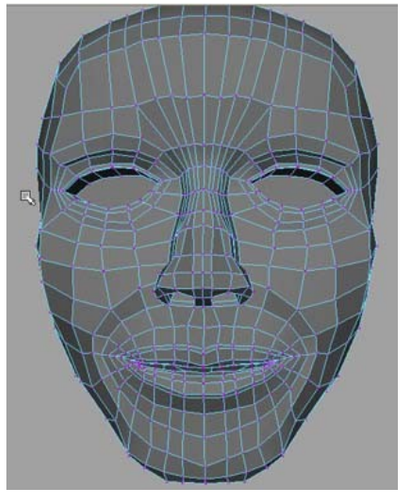
光线
遮盖

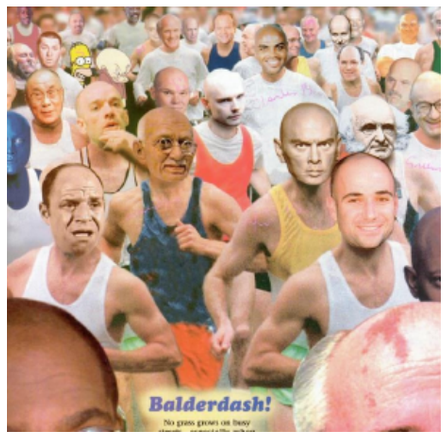
神经网络、特性脸型、局部特征分析

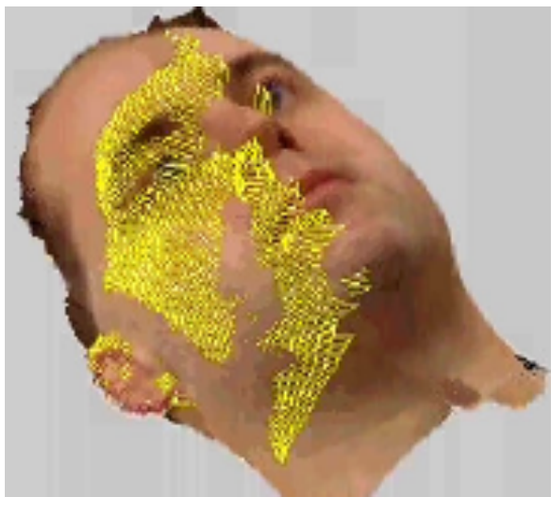
安全
剧场

1996年，政府脸型识别实验（FERET）

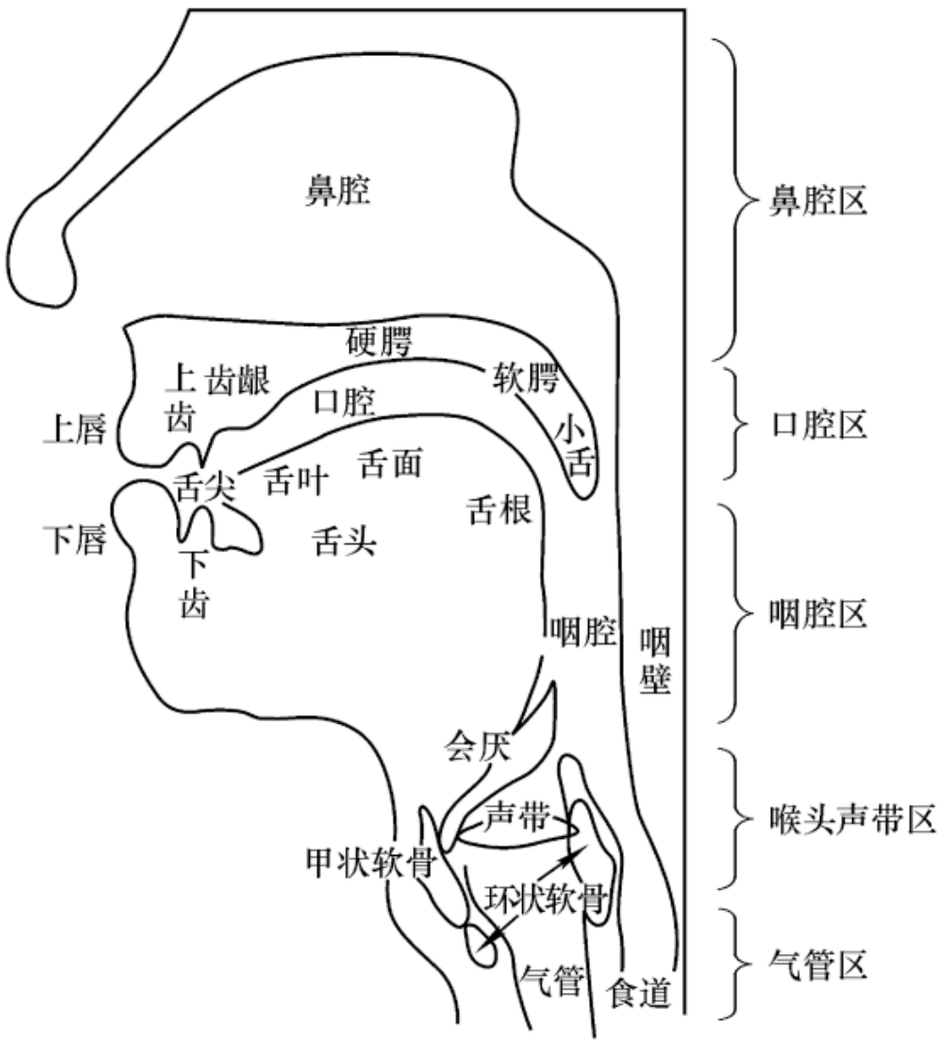
样本小于100个字节，好的大约为86个字节







语音

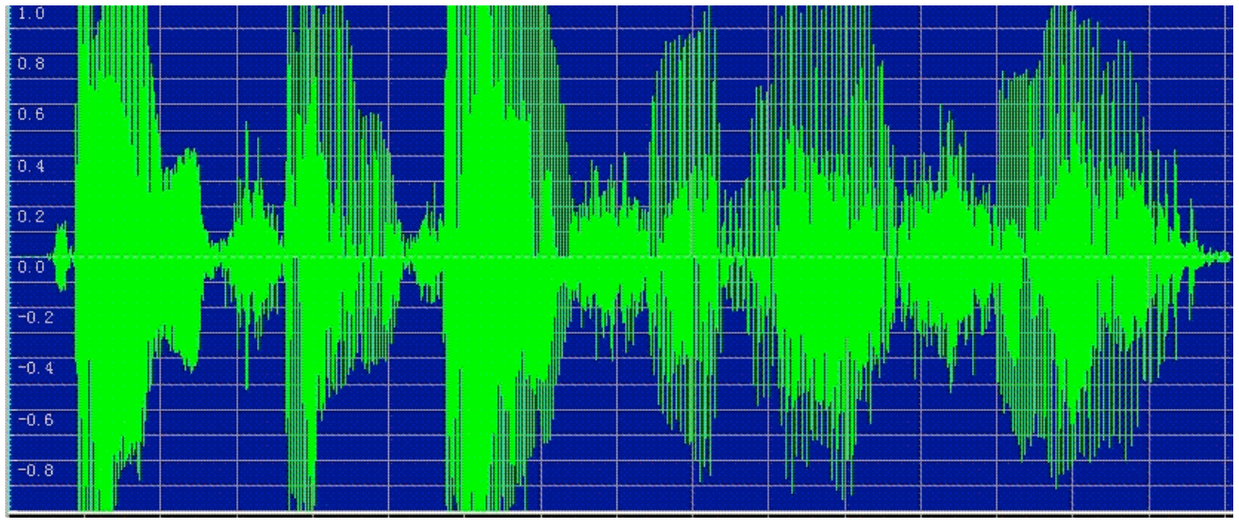


发音器官纵侧面示意图

结合了生理和行为两种成分

语音识别 vs 发生者识别

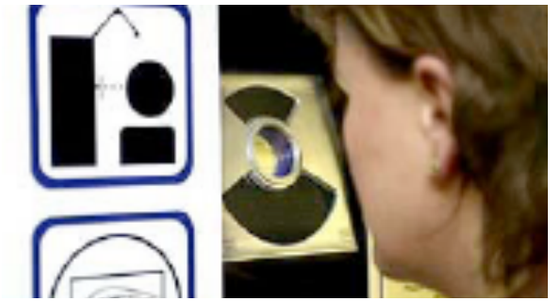
有约束识别 vs 无约束识别



嘈杂环境、没有电话、不够健壮

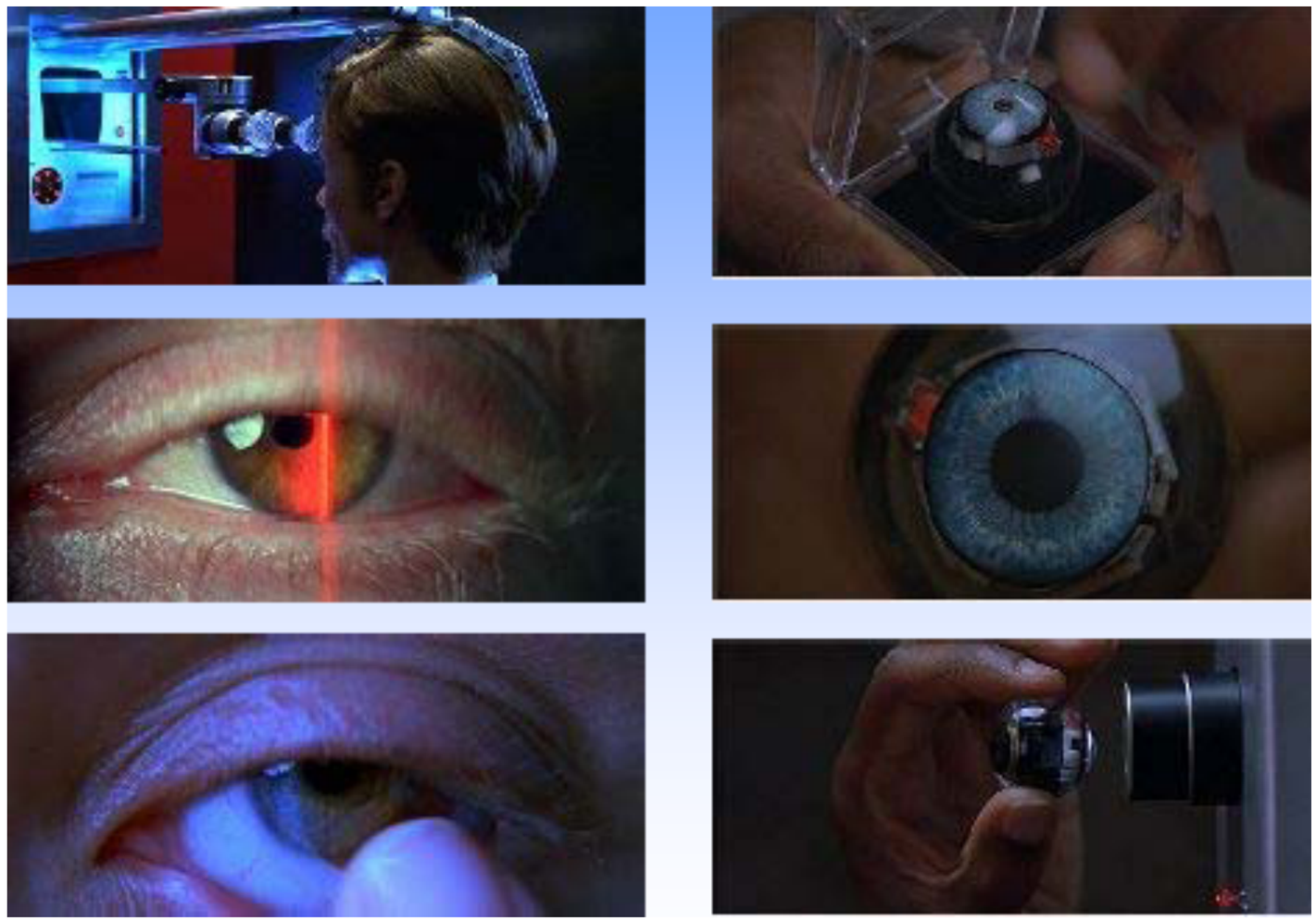
Types of Biometrics

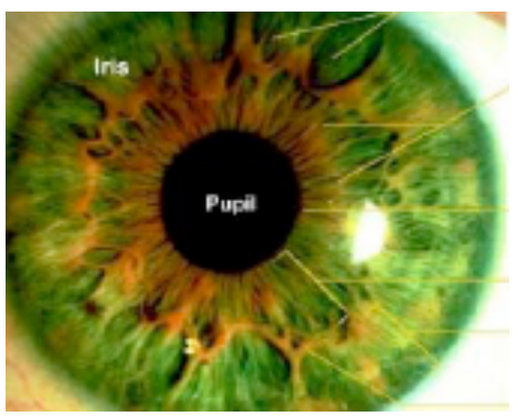
虹膜和视网膜



眼镜

时间





虹膜编码

*256*字节

http://www.cl.cam.ac.uk/~jgd1000/

签名

- 最古老的方式
- 唯一、高效、难于伪造
- 注册验证简单方便
- 错报率高
- 容易被哄骗

- 伪造责任归属
- 卡上签名
- PIN & 电子令牌
- 电子签章

静态 *vs* 动态

- ePadLink
  - 分析速度、压力、加速度、节奏
  - 存储小于1K，每秒40
  - 灵活性好
  - 能扩展到PDA、PC和网络

http://www.epadlink.com/

Types of Biometrics

击键

Brief History of Keystroke Biometrics

WW-II
Military Intelligence identifies the "Fist of the Sender" method

1979
SRI International develops first hardware-based implementation

1984
National Bureau of Standards study finds technology to be 98% effective

1988
Technology found to comply with NIST Computer Security Act of 1987

2000
FSTC/IBG Comparative testing program verifies keystroke technology

2001
Technology embedded into consumer products from cell phones to home security

时间、压力、面积

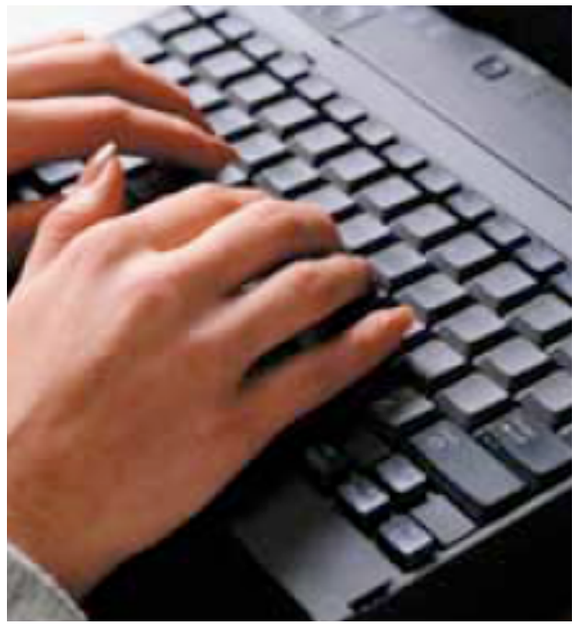
击键监控潜在的威胁已经超过了它的合理性

最自然的应用是“固化”口令

错误率过高，口令太短不行

作者识别
剽窃检测

http://www.biopassword.com/



Types of Biometrics

其他

汗毛孔

握手

和计算机或者智能手机的交互

身体气味

脚印

步态

脑电波分析

生物学认证挑战

如果一个系统是人制作的
那么它也能被人击败

唯一性

生日悖论

持久性


大萌子和萌爸 .1岁
摄影师：萌妈

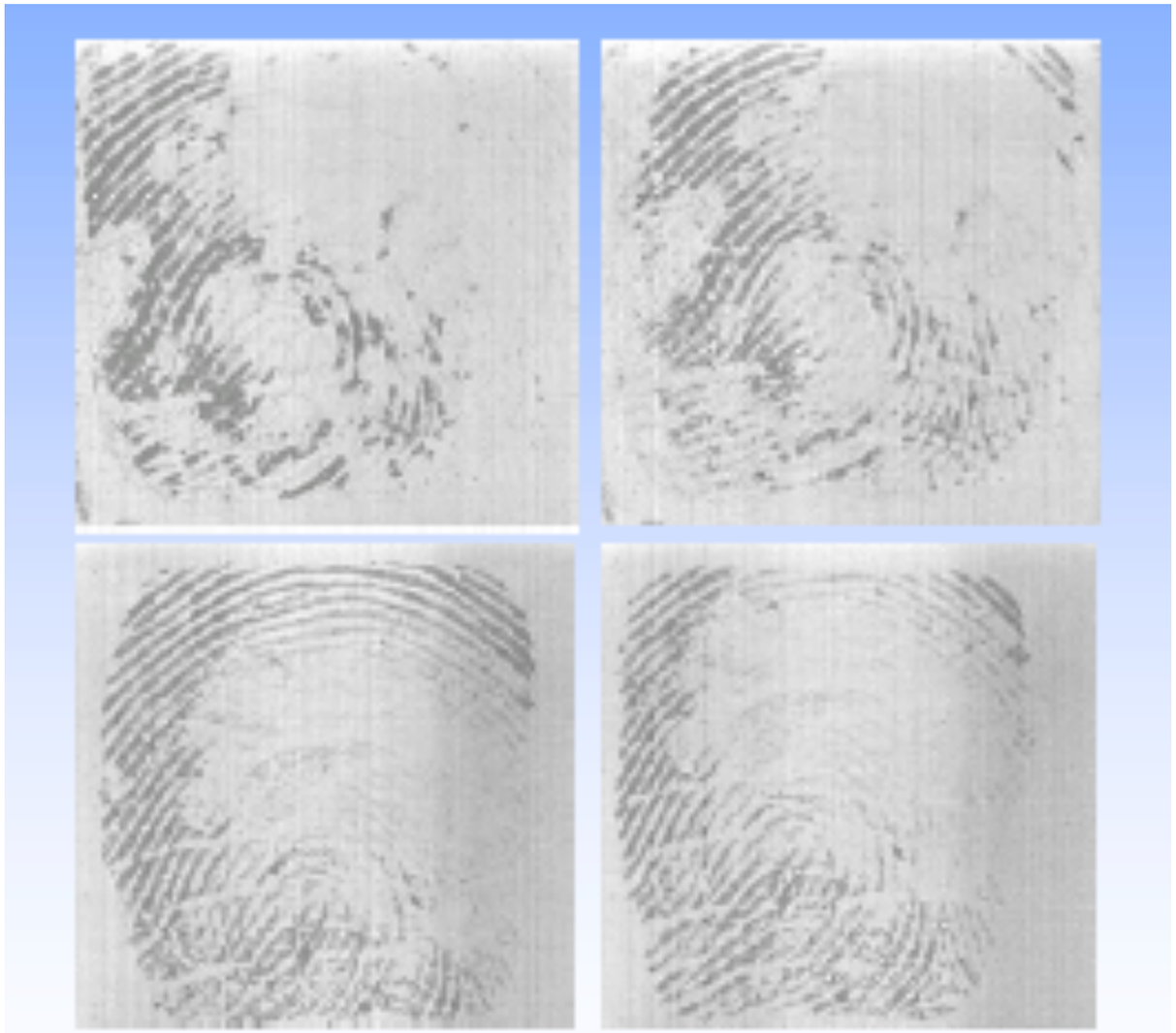

大萌子和萌爸 .5岁
摄影师：萌妈
拍摄地点：外语学院
心爱的爸爸和小豹子。小豹子
在11岁搬家时弄丢了


大萌子和萌爸 .10岁
摄影师：萌妈
拍摄地点：外语学院
贪玩掉进臭水沟，长了一头癞
剃头在家治了2个多月


大萌子和萌爸 .20岁
摄影师：萌妈
拍摄地点：小区大门口
有生以来第一次涂了口红，
是姑姑送的情碧。
爸妈都惊呼：好艳！


大萌子和萌爸 .30岁
摄影师：萌妈
拍摄地点：家庭婚宴

噪音



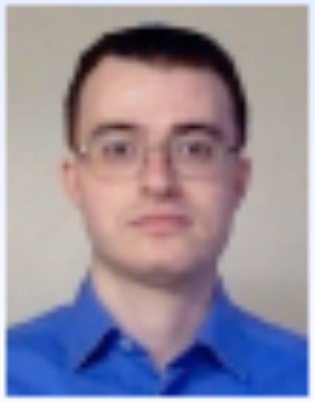
Four impressions of a user's fingerprint

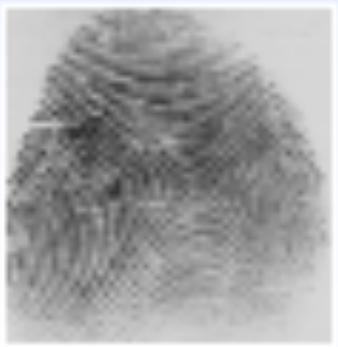
欺骗

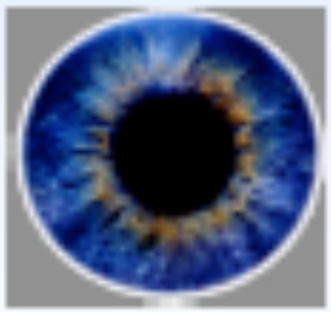
隐私保护

- 老大哥问题
- 匿名权和自由
- 公共安全 vs 公民自由
- 提高了保密性、检验身份、访问控制
- 单一化 vs 多样化
- 未经允许不能泄露

BioKey







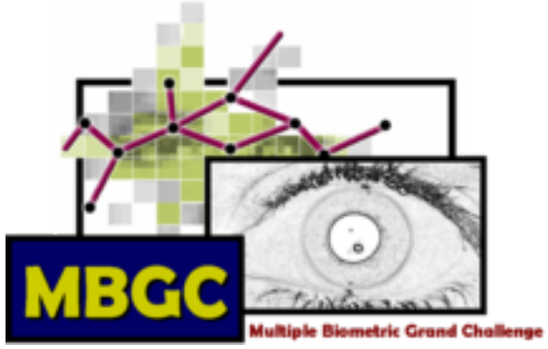
标准化

FIVE

Face In Video Evaluation (FIVE)

FRVT

FACE RECOGNITION VENDOR TEST



OASIS

Biometric Identity Assurance Services

irex IRIS EXCHANGE

Tatt

Tattoo Recognition Technology

https://www.nist.gov/itl/iad/image-group/programsprojects

普适的生物学认证

- 你的物理特征
- 你的行为特征
- 你被感知的位置
- 你使用的硬件和软件
- 你的家庭和好友
- 你在网络上的行为
- … …

Defines You!

Jon Crowcroft

September 24 at 3:38pm · London, United Kingdom ·

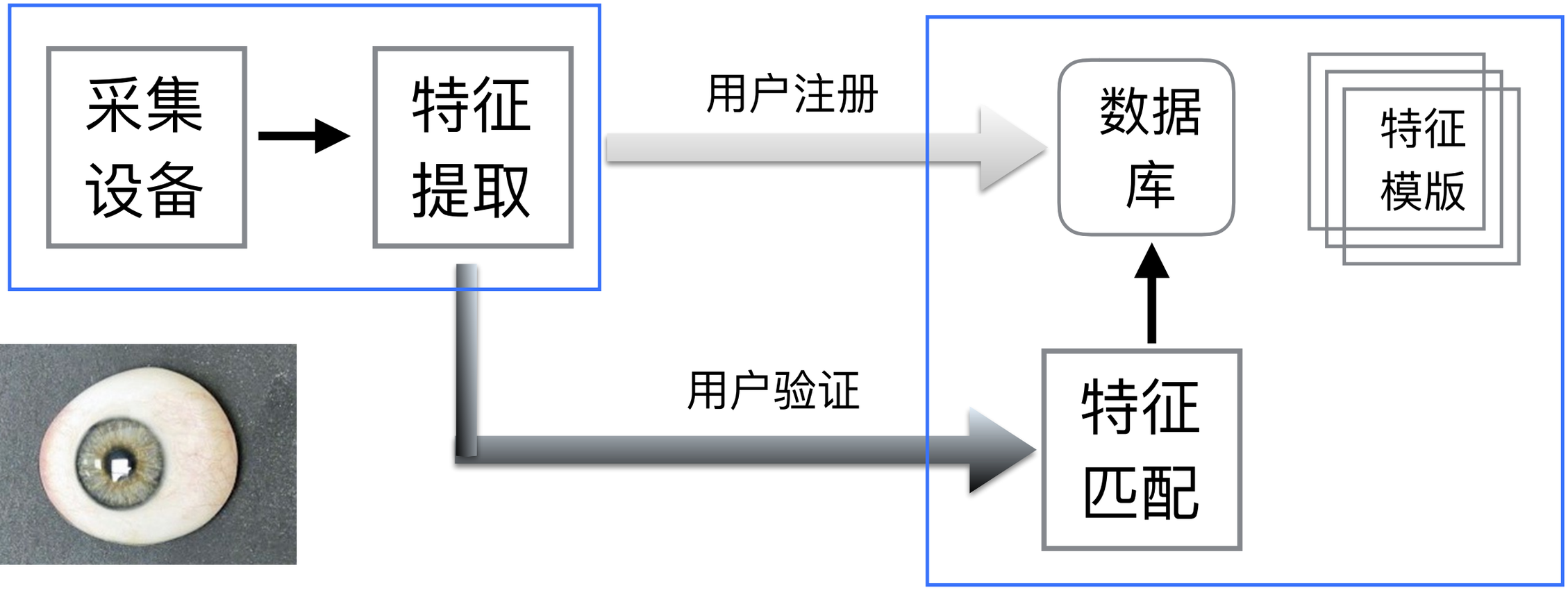
smart phones, smart cars, smart homes, smart cities, smart lights, smart meters, smart clothes, stupid stupid stupid stupid people.

生物学认证验法

如果一个系统是人制作的
那么它也能被人击败

攻击

错误注册	胁迫
共谋	职权滥用



物理攻击	重放攻击	木马攻击	模版攻击
模仿攻击	爬山攻击		
	中间人攻击		

攻击

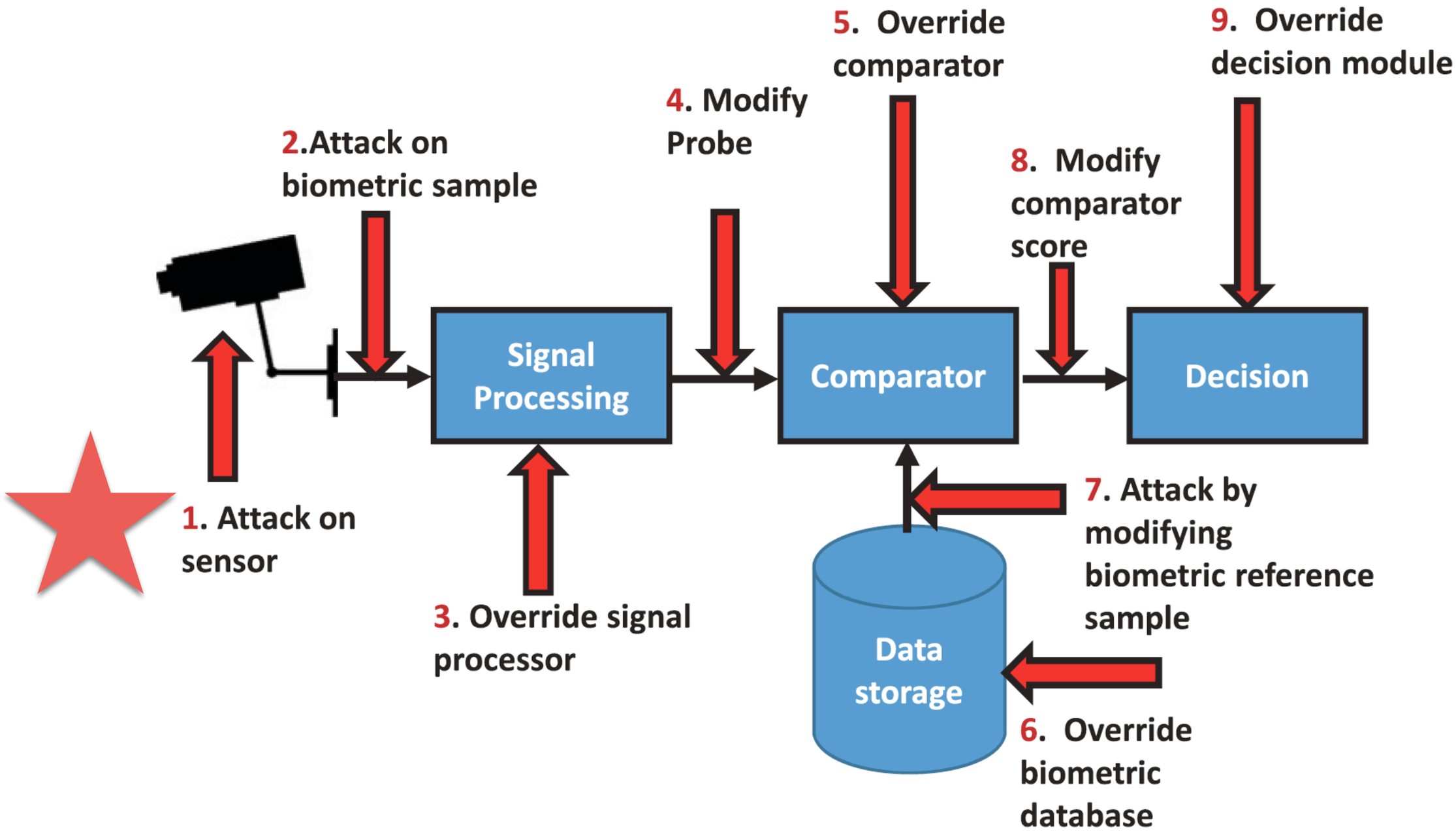
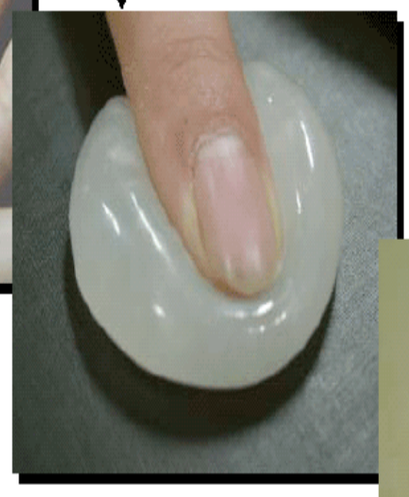


Fig. 1. Vulnerability of a face recognition system (inspired by figure in ISO/IEC 30107-1 [ISO/IEC JTC1 SC37 Biometrics 2016]).

物理攻击

Put the plastic into hot water to soften it.



Press a live finger against it.

The mold

It takes around 10 minutes.

Pour the liquid into the mold.

Put it into a refrigerator to cool.

The gummy finger

It takes around 10 minutes.

人工替代物

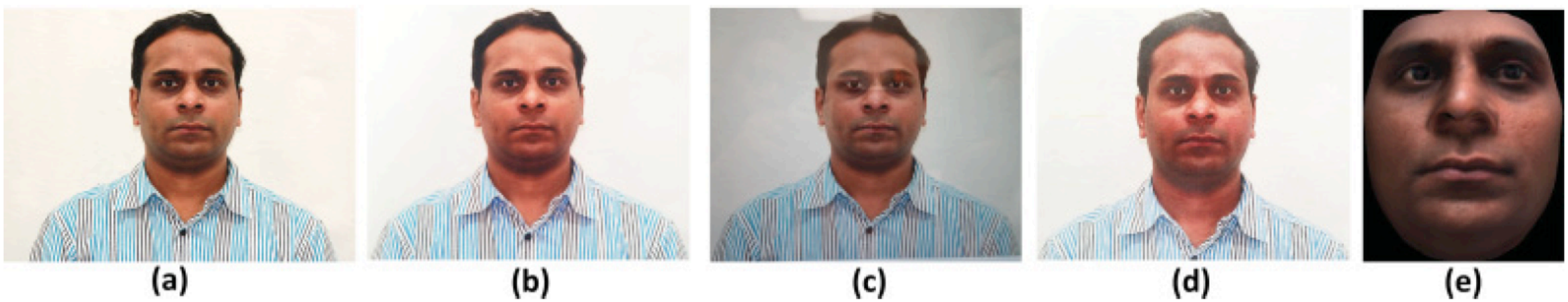


Fig. 2. (a) Bona fide facial image and examples of face artifacts: (b) laser print face artifact; (c) display face photo artifact using an iPad; (d) inkjet print face artifact; (e) 3D face mask.

Fig. 3. Illustration of face artifacts generated using the legitimate user photo obtained from a social website: (a) photo from the social website, (b) inkjet print, (c) electronic display, and (d) laser print.

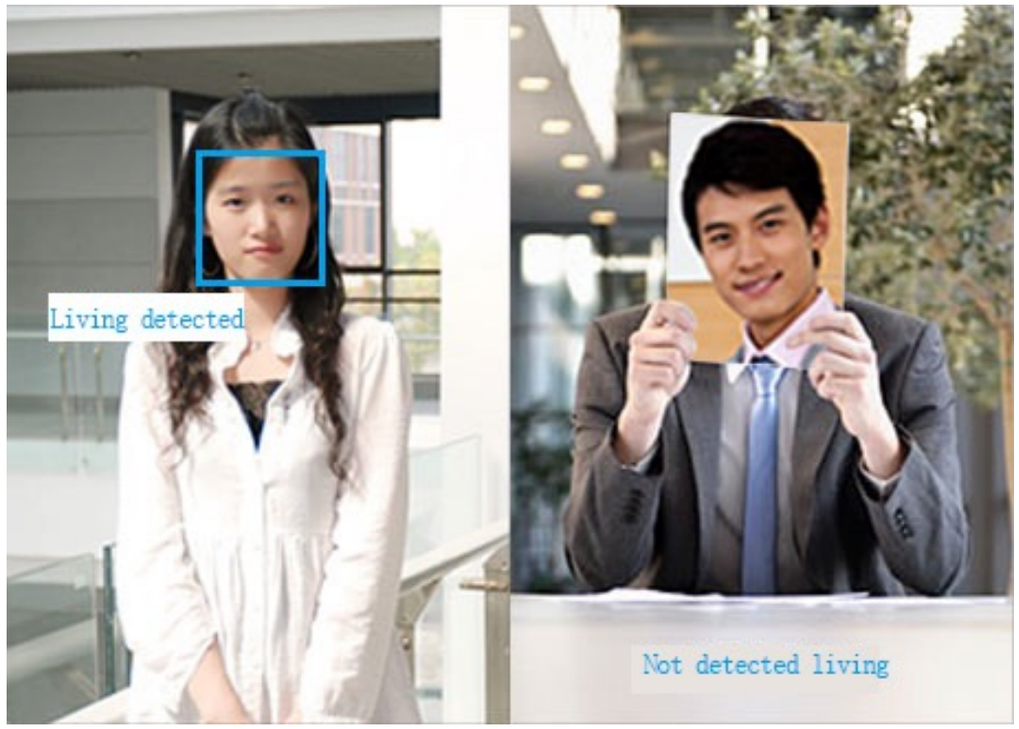
活体检测

- 用户数据获取接口
- 有人监督 vs 无人监督
- 只能降低，不能根除
- 联合采用其余认证技术
- 现有技术

  ✴活体内部固有特性

  ✴分析活体自然产生的特点

  ✴测试身体对外部刺激的反应



人脸验活分类

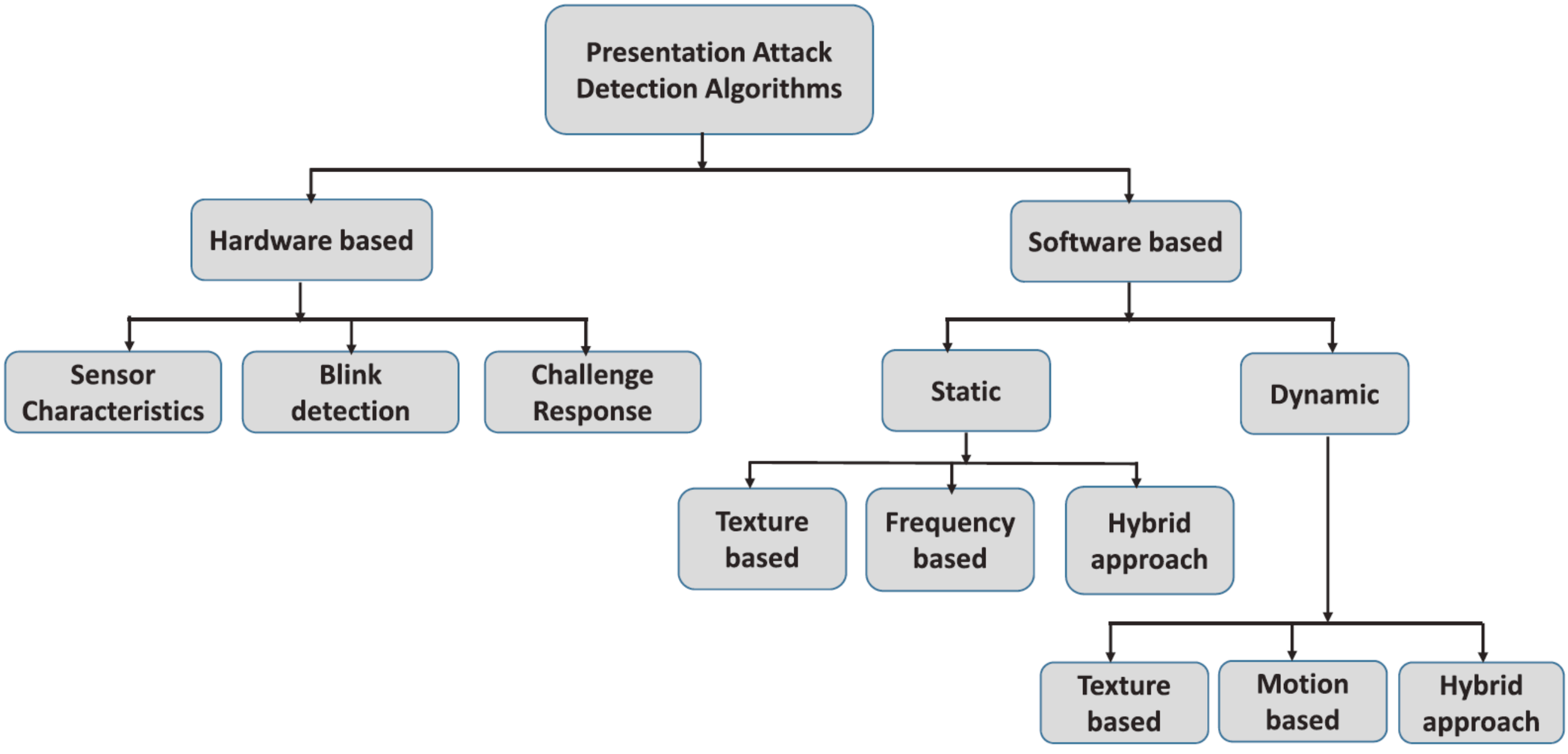


Fig. 6. Classification of face presentation attack detection (PAD) algorithms.

硬件–传感器

Fig. 7. Illustration of using a variation of focus rendered by the LFC to detect face artifacts: (a) real face focus images rendered by the LFC; (b) inkjet print attack focus images rendered by the LFC; (c) display attack using iPad focus images rendered by the LFC; and (d) laser print attack focus images rendered by the LFC

光场相机

多光谱传感器

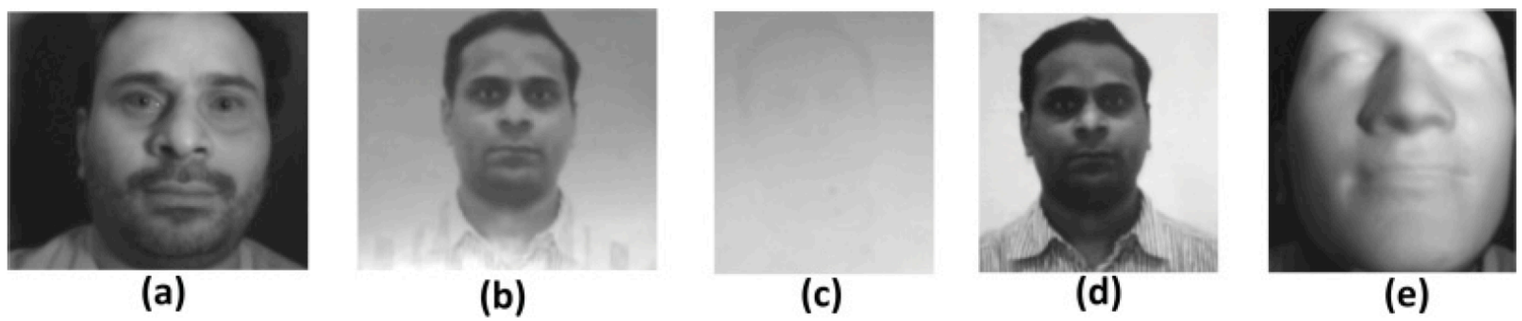
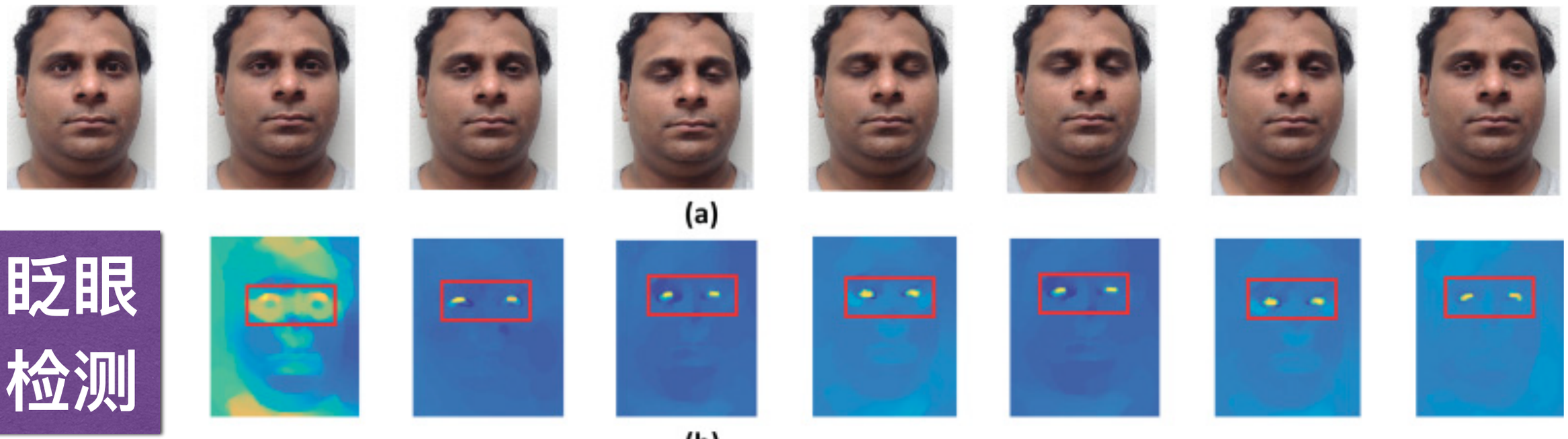


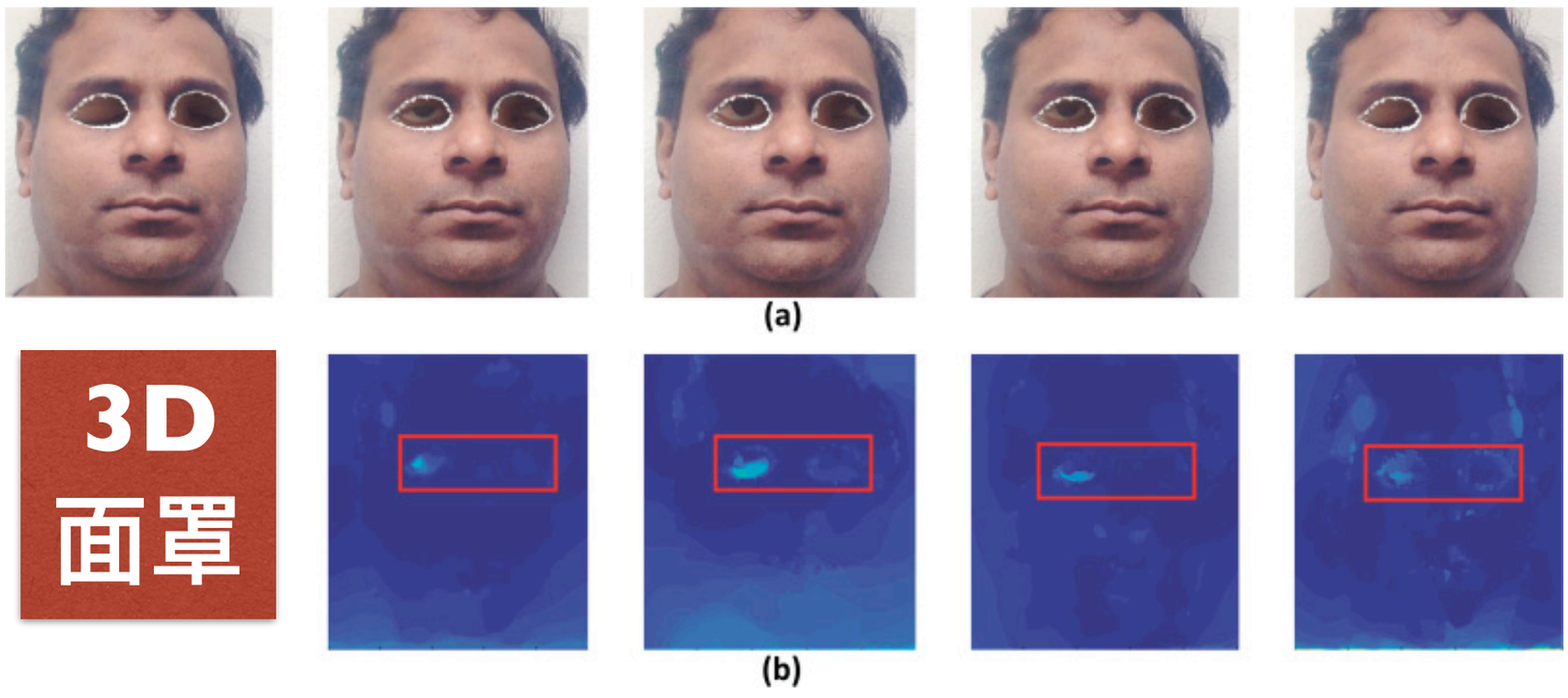
Fig. 8. Illustration of near-infrared face capture of (a) bona fide (real) face; (b) photo print using a laser printer; (c) photo print using an inkjet printer; (d) display attack using an iPad; and (e) 3D mask attack.

硬件

眨眼检测

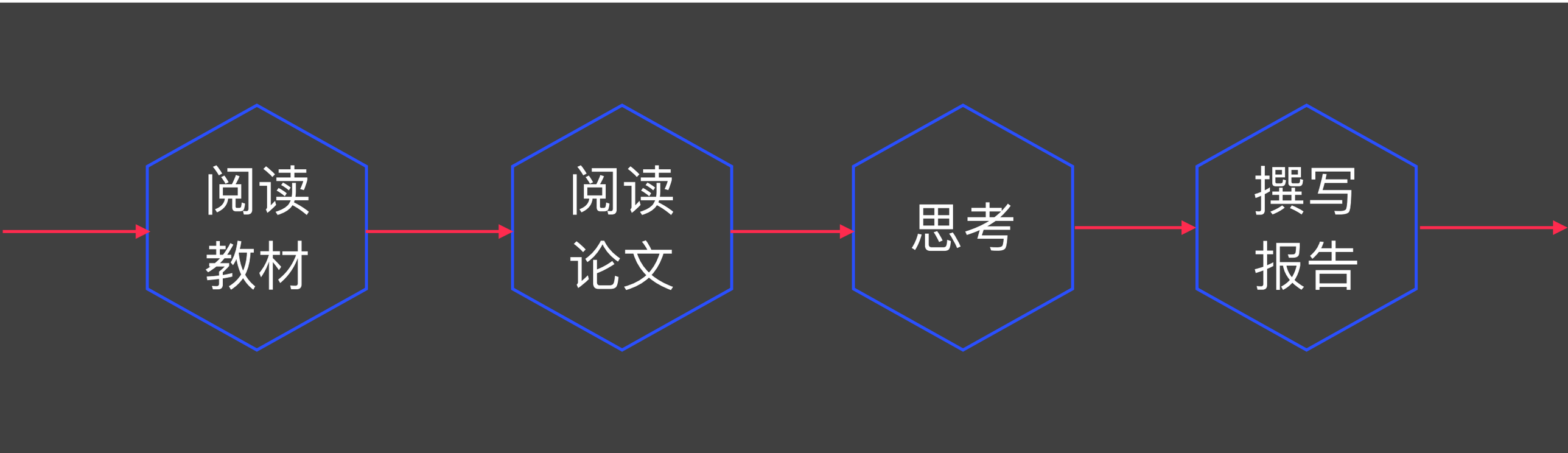


3D面罩



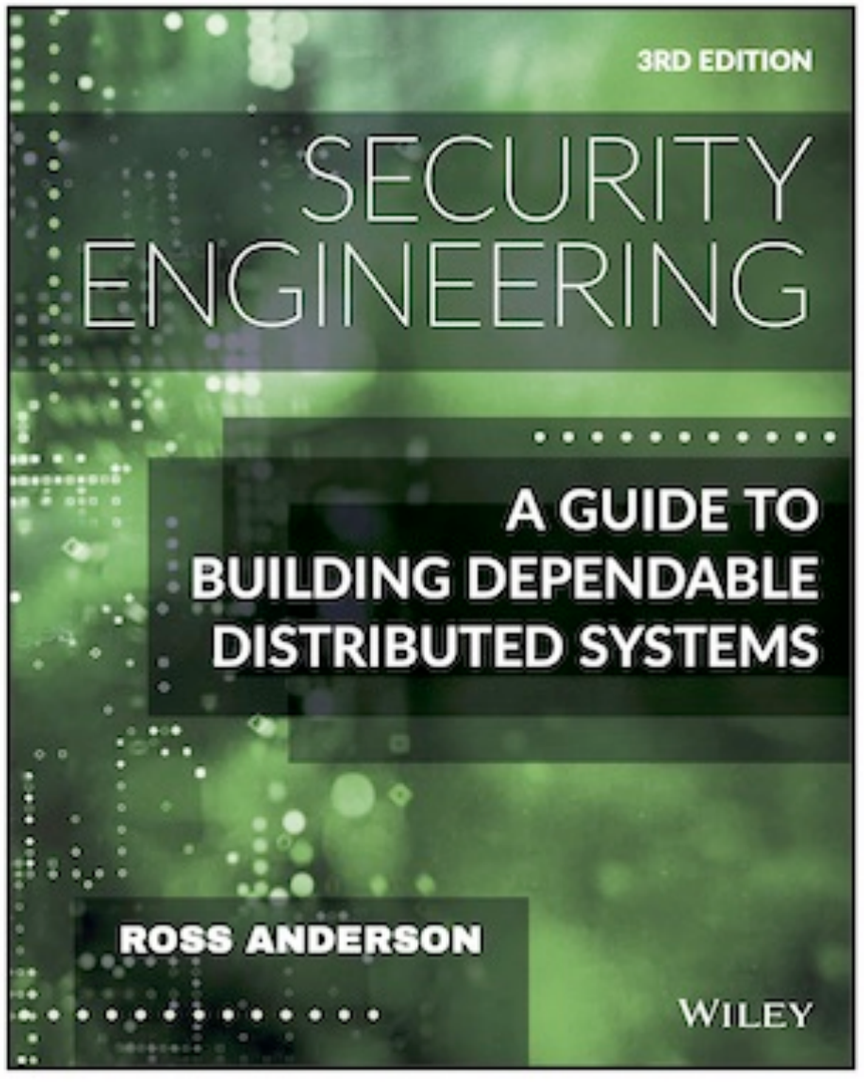
提问时间！

课后作业



Homework

阅读教材



阅读第17章

Homework

课后作业

要求阅读如下文章，写阅读报告

Face Flashing: a Secure Liveness Detection Protocol based on Light Reflections

Di Tang
Chinese University of Hong Kong
td016@ie.cuhk.edu.hk

Zhe Zhou
Fudan University
zhouzhe@fudan.edu.cn

Yinqian Zhang
Ohio State University
yinqian@cse.ohio-state.edu

Kehuan Zhang
Chinese University of Hong Kong
khzhang@ie.cuhk.edu.hk

NDSS'2018

https://www.ndss-symposium.org

检索一篇人脸验活的好文章
好的会议和期刊：参见CCF列表

1、文章概述
2、主要收获
3、存在疑问
4、所思所感
5、一篇论文

周日晚上12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io